

## ALIS ASSESSMENT FINDINGS

There were 18 findings for ALIS; the following are findings in the initial assessment of ALIS:

1. The Disaster Recovery Plan for ALIS is incomplete. Only has one scenario that is the worst-case scenario. (Security Management) \*\*
2. The ALIS Security Plan does not depict the true state of the access controls on ALIS. The controls identified to support I&A mechanisms are not strong enough to support a controlled access protection level. (Security Management) \*\*
3. Lack of strong password composition (I&A compliance)\*\*
4. Passwords are not changed at regular intervals for regular users as well as administrators (I&A Compliance)\*\*
5. Passwords are not monitored for ageing (I&A Compliance)\*\*
6. No user termination procedures in effect (Access control)\*\*
7. No inactivity logoff (Access control)\*\*
8. Stored system passwords are not encrypted (Access control)\*\*
9. Insufficient audit trails in ALIS (Audit)\*\*
10. Insufficient audit trails in Informix (Audit)\*\*
11. No Security Training (Security Training and Awareness)\*
12. No refresher security training (Security Training and Awareness)\*
13. No Rules of Behavior (Security Plan)\*
14. No Certification Statement for ALIS (Security Management)\*\*
15. No Accreditation Statement for ALIS (Security Management)\*\*
16. No Security Test Plan for ALIS (Security Management)\*\*
17. No Banner Pages before access to application (Software Security)\*
18. Both public data and unclassified but sensitive information are on one database. The public accesses database that also has SBU data.

\* Legislation Requirement

\*\* Regulation Requirement